Los enrutadores ASUS se han convertido en el objetivo de una botnet naciente llamada Cyclops Blink, casi un mes después de que se revelara que el malware abusaba de los dispositivos de firewall WatchGuard como un trampolín para obtener acceso remoto a las redes violadas.

Según un nuevo informe publicado por Trend Micro, el *«propósito principal de la botnet es construir una infraestructura para futuros ataques a objetivos de alto valor»,* debido a que ninguno de los hosts infectados *«pertenece a organizaciones críticas, o aquellas que tienen un valor evidente sobre espionaje económico, político o militar».*

Las agencias de inteligencia del Reino Unido y Estados Unidos caracterizaron a Cyclops Blink como un marco de reemplazo para VPNFilter, otro malware que ha explotado dispositivos de red, principalmente enrutadores de oficinas pequeñas y domésticas (SOHO) y dispositivos de almacenamiento conectado a la red (NAS).

Tanto VPNFilter como Cyclops Blink, se atribuyeron a un actor patrocinado por el estado ruso rastreado como Sandworm (también conocido como Voodoo Bear), que también se ha relacionado con una serie de intrusiones de alto perfil, incluido el de los ataques de 2015 y 2016 en la red eléctrica ucraniana grid, el ataque NotPetya de 2017 y el ataque del Destructor Olímpico de 2018 en los Juegos Olímpicos de Invierno.

Escrito en lenguaje C, el botnet modular avanzado afecta a varios modelos de enrutadores ASUS, y la compañía reconoce que está trabajando en una actualización para abordar cualquier posible explotación:

- Firmware GT-AC5300 bajo 3.0.0.4.386.xxxx
- Firmware GT-AC2900 bajo 3.0.0.4.386.xxxx
- Firmware RT-AC5300 bajo 3.0.0.4.386.xxxx
- Firmware RT-AC88U bajo 3.0.0.4.386.xxxx
- Firmware RT-AC3100 bajo 3.0.0.4.386.xxxx
- Firmware RT-AC86U bajo 3.0.0.4.386.xxxx
- Firmware RT-AC68U, AC68R, AC68W, AC68P bajo 3.0.0.4.386.xxxx

- Firmware RT-AC66U_B1 bajo 3.0.0.4.386.xxxx
- Firmware RT-AC3200 bajo 3.0.0.4.386.xxxx
- Firmware RT-AC2900 bajo 3.0.0.4.386.xxxx
- Firmware RT-AC1900P, RT-AC1900P bajo 3.0.0.4.386.xxxx
- RT-AC87U (final de vida útil)
- RT-AC66U (final de vida), y
- RT-AC56U (final de vida útil)

Cyclops Blink, además de usar OpenSSL para cifrar las comunicaciones con sus servidores de comando y control (C2), también incorpora módulos especializados que pueden leer y escribir desde la memoria flash de los dispositivos, lo que le otorga la capacidad de lograr persistencia y sobrevivir a los restablecimientos de fábrica.

Un segundo módulo de reconocimiento sirve como canal para filtrar información del dispositivo pirateado al servidor C2, mientras que un componente de descarga de archivos se encarga de recuperar cargas útiles arbitrarias opcionalmente por medio de HTTPS.

Actualmente se desconoce el modo exacto de acceso inicial, pero se dice que Cyclops Blink afectó a los dispositivos WatchGuard y los enrutadores ASUS ubicados en Estados Unidos, India, Italia, Canadá y Rusia desde junio de 2019.

Algunos de los hosts afectados pertenecen a una empresa de abogados en Europa, una entidad mediana que produce equipos médicos para dentistas en el sur de Europa y una empresa de plomería en Estados Unidos.

Debido a que los dispositivos y enrutadores IoT se están convirtiendo en una lucrativa superficie de ataque debido a la poca frecuencia de parches y la ausencia de software de seguridad, Trend Micro advirtió que esto podría conducir a la formación de *«redes de bots eternas»*.

> *«Una vez que un dispositivo IoT está infectad con malware, un atacante puede*

> *tener acceso a Internet sin restricciones para descargar e implementar más etapas de malware para reconocimiento, espionaje, proxy o cualquier otra cosa que el atacante quiera hacer»,* dijeron los investigadores.

> *«En el caso de Cyclops Blink, hemos visto dispositivos que estuvieron comprometidos durante más de 30 meses seguidos y se configuraron como servidores estables de comando y* control para otros bots».